ELECTRONIC VOTING PROCESS USING FAIR BLIND SIGNATURES

The present invention concerns the field of cryptography and, more especially, the present invention relates to electronic voting.

Unlike traditional voting, which involves voters casting their votes by physical attendance at a polling station, electronic or "on-line" voting enables voters to cast their respective votes remotely with the aid of a suitable machine (computer, mobile telephone, etc.) connected to a network such as the Internet.

It is to be understood that in the present document, unless the context requires otherwise, the expressions "on-line voting" and "electronic voting" will be used interchangeably.

In order for an on-line voting system to constitute an acceptable alternative to traditional voting schemes, it is generally considered necessary for the on-line system to respect the following principles:

- **Eligibility**: only votes of legitimate voters must be taken into account;
- **Unreusability**: each voter must only be able to cast one vote;
- **Anonymity**: the ballot must be secret, in other words, it should be impossible to tell how a particular voter has voted;
- **Accuracy**: once a ballot has been cast it should be impossible to alter it;
- **Fairness**: it should only be possible to tally up the results of the vote after all votes have been cast (in other words, it should be impossible to perform partial tabulation while voting is still in progress);
- **Vote and walk-away**: Once a voter has cast his vote there is no further action he need take;
- **Public verifiability**: the validity of the whole voting process can be readily verified by anyone.

Many studies have attempted to design secure and convenient electronic voting systems. Indeed, electronic voting is one of the major applications of cryptography. The known proposals for electronic voting schemes often make use of blind signatures.

A digital signature scheme is a cryptographic protocol involving a user and a signer. The user generates a message, generally for transmission over a network, such as the Internet. The signer applies a digital signature to the message as an indication of the validity or authenticity of the message. In conventional digital signature schemes the signer knows the content of the message to which the digital signature is being applied, an algorithm (e.g. the well-known RSA algorithm) is used to generate a digital signature which is difficult or impossible to forge, and the validity of the digital signature can be verified by any interested third party simply by applying the signer's public key.

In a blind signature scheme, the user can obtain a digital signature on his message without letting the signer have information on the content of the message. Clearly this is a desirable feature in a voting application where the message being signed corresponds to a vote. A well-known blind signature scheme developed by Prof. Dr. David Chaum is described in EP-A-0 139 313. Blind signature schemes are often proposed for use in digital cash applications so as to enable an individual to purchase digital cash from a financial institution in a manner which prevents the financial institution from being able to trace the subsequent use of that cash.

As indicated above, various electronic voting schemes have been proposed that make use of blind signatures. However, these earlier proposals suffer from a number of drawbacks. Some schemes do not satisfy the requirement for "vote and walk-away", instead each voter must participate in the vote counting procedure after all voters have cast their votes. In some schemes, if the "vote and walk-away" principle is respected then the "accuracy" principle is not.

The preferred embodiments of the present invention provide an efficient and secure electronic voting scheme based not on ordinary blind signatures but on fair blind signatures.

In an ordinary blind signature scheme, if the signer signs a number of documents for different users then, when he is presented with one particular document that he has signed, he will not be able to determine when or for whom he signed that document. By way of contrast, in a fair blind signature scheme (FBSS), there is an additional participant, one or more trusted authorities (or "judges"), and the signer can identify which signature resulted from a given signing session with the help of the trusted authority (or of a quorum of trusted authorities if there is more than one).

If the signer has a transcript of a particular signing session then he can identify the signature-message pair resulting from that session: this is termed "signature tracing". Conversely, if the signer has available a particular signature-message pair then he can determine the signing session at which this was generated: this is termed "session tracing". Although fair blind signature schemes enable a given digital signature to be linked to a given user, generally the user's message still remains private. Fair blind signature schemes have mainly been proposed in the context of the fight against organized crime, particularly, the prevention of money laundering.

The preferred embodiments of the present invention provide an electronic voting scheme which uses a fair blind signature process to overcome the drawbacks of the prior art, which respects the above-mentioned principles of anonymity, eligibility, unreusability, accuracy, fairness, vote and walk-away and public verifiability, which is efficient and secure.

The present invention provides an electronic voting method comprising the step of using a fair blind signature scheme to obtain a digital signature of a signal containing the voter's vote. Typically, the digital signature will be applied by a server module that can be designated an "admin server" module.

In the preferred embodiments of the present invention the fair blind signature scheme is a threshold fair blind signature scheme in which the blind signature is generated by the cooperation of t out of n admin servers and the voter associated with a particular ballot (but not the way in which he has voted), can be identified by the cooperation of r out of n trusted authorities.

Advantageously, each digital signature obtained from the set of admin servers is one-more unforgeable as long as $n - t + 1$ of the servers in said group are honest.

In general, the signal that is signed by the admin server module corresponds to the voter's vote encrypted according to a first encryption scheme (notably, that of a tallier module used to tally up the votes cast). So, in this case, the electronic voting method will further comprise the step of applying the decryption scheme inverse to said first encryption scheme to the data signal so as to retrieve the voter's vote. Preferably the tallier module is implemented as a mix-net.

According to the preferred embodiments of the present invention, the data signal comprising the voter's encrypted vote is itself encrypted, according to a second encryption scheme (notably, that of a randomizing module) and it is this encrypted data signal that is transmitted to an electronic ballot box as the voter casting his vote. Advantageously, a batch of the encrypted data signals is supplied to the randomizer module for decryption and reordering (so that the voter's identity cannot be determined by consideration of the position of his vote in the list of cast votes). Preferably, the randomizer module is a mix-net.

In the above-described electronic voting method according to the preferred embodiments of the present invention, the mix-net servers do not normally need to produce proofs of correctness of their operation (confirming that the outputs thereof truly do correspond to re-ordered ones of their inputs). Such proofs are only required in the case where a discrepancy is noticed in the voting process. For this reason, in the case of an honest vote (where no voter or mix-net server cheats), the counting of votes is extremely rapid.

Further features and advantages of the present invention will become apparent from the following description of a preferred embodiment thereof, given by way of example, as illustrated by the accompanying drawings, in which:

Fig. 1 is a diagram indicating schematically the main participants in the electronic voting scheme of a preferred embodiment of the present invention;

Fig. 2 is a diagram illustrating schematically the main steps in the vote-casting phase of the preferred embodiment of the electronic voting method according to the present invention;

Fig. 3 is a flow diagram illustrating the main steps in the vote-counting phase of the preferred embodiment of the electronic voting method according to the present invention;

Fig. 4 is a flow diagram indicating the main steps in a procedure for handling discrepancies noted during the counting phase, particularly in the case where the discrepancy is attributable to a server in a randomizing mix-net; and

Fig. 5 is a flow diagram indicating the main steps in a further procedure for handling discrepancies noted during the counting phase, particularly in the case where the discrepancy is attributable to a voter.

The electronic voting method of the present invention involves participants of six basic types:

- voters,
- an admin server or "electoral authority" (preferably implemented using a set of admin servers),
- a randomizing entity (preferably implemented as a randomizing mix-net),
- a ballot-box server,
- talliers (which are preferably tally servers of a tallier mix-net), and
- a number, n, of trusted authorities (or "judges").

A given voter can be designated using the symbol $\mathtt{V_i}$ and has an identifying code which can be designated $\mathtt{Id_i}$. A given voter $\mathtt{V_i}$ can apply a certificate, $\mathtt{C_i}$, to data he transmits so as to indicate his entitlement to participate in a given voting process.

Fig.1 is a diagram illustrating schematically how the various participants interact in one preferred embodiment of the present invention.

As shown in Fig. 1, according to the electronic voting scheme of the preferred embodiment of the present invention, voters, 10, make contact with an admin server module 20 in order to obtain digital signature of encrypted vote data, according to a fair blind signature scheme (FBSS). The digitally-signed vote data is provided to a bulletin board server 30 when the voter casts his vote. This vote data is doubly-encrypted: the outer layer of encryption is according to an encryption scheme of a randomizer module 40, the inner layer of encryption is according to an encryption scheme of a tallier module 50. The randomizer module 40 decrypts the vote, leaving it in (singly-)encrypted form, and randomizes the order of the votes received from different voters. The tallier module 50 decrypts the (singly-)encrypted, and re-ordered votes so as to retrieve the votes that have been cast, tallies up the votes and outputs the results of the vote.

The admin server module (20) maintains a database, L_{AS}, of data received from voters for whom it has provided digital signatures. The bulletin board server (30) maintains a database, L_{BB}, of data received from voters who have posted votes.

At various stages in the voting process discrepancies (or “irregularities”) can be detected (for example, at the bulletin board server 30, the randomizer module 40 or the tallier module 50). If the irregularity is determined to be attributable to the voter, the set of trusted authorities, 60, appointed to help operate the fair blind signature scheme are contacted so as to be able to determine the (singly-) encrypted vote data and associated digital signature data affected by the irregularity. In the case where the randomizer module 40 is implemented as a mix-net, it is only necessary for the mix-net servers to generate proofs of correctness (notably, zero-knowledge proofs of correctness) in the case where an irregularity is detected in the voting process. If no irregularities are detected in the voting process then there is no need for the mix-net servers of the randomizer module 40 to generate proofs of correctness. This renders the electronic voting process according to the preferred embodiment of the present invention fast in producing the results of the vote.

The voting method according to the preferred embodiment of the present invention involves the following cryptographic primitives: a digital signature scheme (applied by the voter, 10), a threshold fair blind signature scheme (involving the voter, an admin server module 20 implemented using a set of admin servers and the set of trusted authorities 60), two mix-nets (one mix-net implementing the randomizing module 40, and one mix-net implementing the tallier module 50), and two encryption schemes (that of the randomizing mix-net 40 and that of the tallier mix-net 50).

In the description below of the electronic voting process according to a preferred embodiment of the invention, the cryptographic primitives that are used will be referred to in general terms, without giving full details of any particular implementation. This is because the present invention is not limited with regard to the particular way in which these various primitives are put into practice. Numerous digital signature schemes, threshold fair blind signature schemes, mix-nets and encryption schemes are well-known in the field of cryptography and any secure implementation of these is suitable for use in the present invention.

In a similar way, the present invention is applicable without limitation with regard to the particular hardware or software that is used to implement the various described functions. Suitable software routines and hardware will readily occur to the skilled man based on his common general knowledge in this field.

The voting method according to one preferred embodiment of the present invention will now be described with reference to Figs. 2 to 5. This voting method has three main phases: a registration phase, a voting phase, and a vote-counting stage.

The registration phase involves the voter, $\mathbf{V}_i$, interacting with an admin server, **AS**, or electoral authority, in order to activate his entitlement to vote. As a result of this interaction, the admin server adds this voter, $\mathbf{V}_i$, to its electoral register of voters able to participate in future elections. The interaction between the voter and the admin server during the registration phase can take any convenient form. The voter may contact the admin server directly, for example, by electronic means, or indirectly, for example by using a telephone-based voice-activated response system or by mailing in a completed form to an electoral officer who then updates the electoral list held by the admin server. Advantageously, some security measures, of any convenient type, are adopted so as to ensure that only people who are truly entitled to vote can become recorded in the admin server's electoral register.

During the registration phase the voter obtains the certificate, $\mathbf{C}_i$, that permits him to sign messages. This certificate can take any convenient form: for example, it could be an X509 certificate. The certificate, $\mathbf{C}_i$, is used by the voter during the voting phase.

The voting phase of the preferred embodiment of electronic voting method according to the present invention will now be described with reference to the flow diagram of Fig. 2.

A voter, $\mathbf{V}_i$, selects the vote of his choice, $\boldsymbol{v}_i$, and encrypts this vote using the encryption key of a tallier, namely an entity that will be involved in tallying the results of the voting process. Any convenient asymmetric algorithm (RSA, El Gamal, etc.) can be used as the encryption scheme of the tallier.

In the preferred embodiments of the invention the tallier is implemented as a mix-net, **TM** , consisting of a sequence of servers (or "mixes"). Each server of the mix-net receives a batch of input messages and produces as output the batch in a permuted order. The tallier mix-net can be of various types, for example, a Chaumian mix-net (that is, a mix-net in which the messages are successively encrypted with each server's key), a re-encryption mix-net (where there is a single key for all servers in the mix-net, but randomized re-encryption in each server) etc. Preferably the tallier mix-net is a simple mix-net but it is robust (that is, if one tallier server is unavailable, it is possible to replace it by another one).

The process whereby the voter encrypts his vote using the encryption key of the tallier mix-net, **TM**, can be represented, as follows:

$$x_i = \mathbf{E}_{\mathrm{TM}}\,(\boldsymbol{V}_{\mathrm{i}})$$

where x_i is the encrypted vote and $\mathbf{E}_{\mathrm{TM}}$ represents the application of the encryption scheme of the tallier mix-net, **TM**.

The voter, $\mathbf{V}_{\mathrm{i}}$, then blinds the encrypted vote, x_i, as follows:

$$e_i = \mathbf{FB}\,(x_i\,,r_i)$$

where **FB** represents the application of the blinding procedure, and r_i is a randomly chosen blinding factor.

The voter, $\mathbf{V}_{\mathrm{i}}$, signs the blinded and encrypted vote, e_i, as a gauge of its authenticity, using his digital signature scheme, $\mathbf{S}_{\mathrm{i}}$. That is, the voter generates

$$s_i = \mathbf{S}_{\mathrm{i}}\ (e_i)$$

The voter, $\mathbf{V}_{\mathrm{i}}$, then sends the data ($\mathbf{Id}_{\mathrm{i}}$, $\mathbf{C}_{\mathrm{i}}$, e_i, s_i) to the admin server, **AS**.

The admin server, **AS**, checks that the signature, s_i , is valid, and that it comes from a voter who is listed in its electoral register (this check being performed by verifying the validity of the certificate $\mathbf{C}_{\mathrm{i}}$). The admin server also checks that this voter has not already voted. The latter check involves determining whether or not the admin server, **AS**, has already generated a digital signature for this voter, $\mathbf{V}_{\mathrm{i}}$, in the current election.

If these checks yield a satisfactory result then the admin server, **AS**, signs the blinded and encrypted vote, e_i, as a gauge of its authenticity, using its digital signature scheme, $\mathbf{S}_{\mathrm{AS}}$. That is, the admin server generates:

$$d_i = \mathbf{S}_{\mathrm{AS}}\ (e_i)$$

The admin server transmits d_i back to the voter, $\mathtt{V_i}$.

The admin server, **AS**, keeps a record of the data ($\mathtt{Id_i}$, $\mathtt{C_i}$, e_i, s_i) received from all of the voters for whom it emits digital signatures during the voting process. At the end of the voting phase, the admin server, **AS**, announces the number of voters for whom it has signed votes, and publishes a list L_{AS} = ($\mathtt{Id_i}$, $\mathtt{C_i}$, e_i, s_i) including the data received for all of these voters.

When the voter, $\mathtt{V_i}$, receives back d_i, that is his blinded ballot signed by the admin server, he retrieves a digitally-signed version (y_i) of his ballot (x_i) by unblinding d_i, as follows:

$$y_i = \mathrm{UFB}\ (d_i)$$

where UFB represents the application of the unblinding procedure.

The voter, $\mathtt{V_i}$, then uses the encryption key, $\mathbf{E_M}$, of a randomizing entity to encrypt data (x_i , y_i) corresponding to his encrypted vote and the version of his encrypted vote that is signed by the admin server, **AS**, as follows:

$$c_i = \mathbf{E_M}\ (x_i, y_i)$$

Advantageously, this randomizing entity is a mix-net, **M**, which, once again, preferably is a simple but robust mix-net that can be implemented as a Chaumian mix-net, a randomizing mix-net, etc.

The voter then signs this encrypted data using his signature function, $\mathtt{S_i}$, to generate a signed message σ_i where:

$$\sigma_i = \mathtt{S_i}\ (c_i)$$

The voter then completes his vote by sending data ($\mathtt{Id_i}$, $\mathtt{C_i}$, e_i, σ_i) to an electronic ballot box, **BB**. This electronic ballot box is conveniently presented as a bulletin board and implemented as a web server (or the like). The bulletin board verifies the validity of the signature σ_i and, if it is valid, records the data ($\mathtt{Id_i}$, $\mathtt{C_i}$, e_i, σ_i) supplied in this transmission. Preferably, this data is recorded by the web server (or the like) in a form that is resistant to later modification (for example in a read-only-memory).

When the voting process has ended (i.e. after the polls have closed), the bulletin board, **BB**, publishes a list L_{BB} = ($\mathtt{Id_i}$, $\mathtt{C_i}$, e_i, σ_i) of all data that has been posted during the voting phase in transmissions with valid voter signatures. This list L_{BB} is compared by the admin server with the list of data L_{AS} it generated in relation to all digital signatures it has provided during the voting phase. If there is an entry ($\mathtt{Id_i}$, $\mathtt{C_i}$, e_i, s_i) in L_{AS} for which there is no corresponding entry ($\mathtt{Id_i}$, $\mathtt{C_i}$, e_i, σ_i) in L_{BB} this means that a voter has obtained a blind digital-signature on his encrypted vote but did not cast the vote. Steps are then taken to process e_i so that the corresponding message-signature pair (x_i, y_i) can be determined. In particular, the trusted authorities (or judges) are contacted for help in processing e_i.

According to the preferred embodiment of the invention, if there are n trusted authorities, it is not necessary for the full set, $\mathtt{J}$, of these trusted authorities to cooperate in processing e_i. Cooperation of a sub-set of the trusted authorities (i.e. a number t, where $t < n$) is sufficient. In this way, the scheme is workable even if one, or a small number of, the trusted authorities $\mathtt{J}$ cannot be reached at a given time, or refuses to cooperate. This sub-set of the trusted authorities applies the signature tracing algorithm, $\mathbf{REV}_{\mathtt{J}}$, of the fair blind signature scheme that is being used in the voting process, as follows:

$$f_i = \mathbf{REV}_{\mathtt{J}}\,(e_i)$$

it will be recalled that e_i is the blinded version of voter $\mathtt{V}_\mathtt{i}$'s encrypted vote x_i.

Depending upon the particular fair bind signature scheme that is applied, the retrieved data, f_i, can be the message–signature pair (x_i, y_i) itself. In the following description it will be assumed that the retrieved data f_i is the message–signature pair (x_i, y_i). The retrieved message-signature pair data is recorded in a list, RL, which can be termed a "revocation list" which, preferably, is available for public inspection later on. It should be noted that the retrieved data does not reveal the voter's vote, only an encrypted version thereof. Thus, the voter's privacy is respected.

The counting phase of the electronic voting process according to the preferred embodiment of the present invention will now be described with reference to the flow charts of Figs. 3 to 5.

As indicated in Step 1 of Fig. 3, the list of c_i values recorded by the bulletin board server is supplied to the randomizer module, $\mathtt{M}$, which applies its decryption scheme, $\mathtt{D}_\mathtt{M}$, in order to retrieve signature-message pairs (x_i, y_i). It will be recalled that, in the preferred embodiments of the present invention the randomizer module is implemented as a mix-net. This mix-net outputs a list, $\mathtt{L}$, of the values (x_i, y_i) in a random order, different from the order of receipt of the corresponding values, c_i. The list, $\mathtt{L}$, is then supplied to the tallier module, $\mathtt{TM}$, which is also implemented as a mix-net in the preferred embodiment of the invention.

As indicated in Step 2 of Fig. 3, the tallier mix-net checks the list L for any duplicate entries. This check can be made by the tallier mix-net itself or by another module which cooperates with the tallier mix-net. If any duplicate entries are found this is a discrepancy which represents an irregularity in the voting procedure. A discrepancy-tracing procedure is then invoked, which will be discussed below in connection with Fig. 4. Otherwise, if there are no duplicate entries in the list, L, the tallier mix-net proceeds to Step 3 of Fig. 3, where it checks the validity of the digital signatures y_i of the entries in list L. If any of the digital signatures, y_i, are invalid then, once again, the discrepancy-tracing procedure of Fig. 4 is invoked.

In the case where the tallier determines that all of the digital signatures, y_i, are valid, it next performs a comparison of the entries (x_i, y_i) in L with the entries (x_i, y_i) in the revocation list, RL (see Step 4 of Fig. 3). If there is overlap between the two sets of entries, in other words if L $\cap$ RL is not the empty set, then the discrepancy-tracing procedure of Fig. 4 is invoked. Otherwise, the servers, TM_j, of the tallier mix-net reveal their private keys so that the signals, x_i, can be decrypted (using SK_{TM}). Accordingly, the votes, v_i, are revealed, the tallier module tallies them up then publishes the result of the election (see Step 6 of Fig. 3). The counting stage then ends.

As indicated above, in the case where the checks performed by the tallier module in steps 2, 3 or 4 reveal a discrepancy, the origin of the discrepancy is sought using the discrepancy-tracing of Fig. 4.

According to the discrepancy-tracing procedure of Fig. 4, it is first checked whether the discrepancy arises with the servers of the randomizer mix-net, M. This check is performed by prompting each of the mix-servers, M_j, to generate a zero-knowledge proof of correctness to demonstrate the correspondence between their output and input, using the queried data pair $(x_i, y_i)_q$ as input and applying the mix-net's back-tracing algorithm. Incidentally, if the discrepancy-tracing procedure is being invoked because the tallier found one or more duplicate entries in the list, L, then the queried data pairs $(x_i, y_i)_q$ will be the duplicated entries. If the discrepancy-tracing procedure is being invoked because the tallier found one or more invalid digital signatures, y_i, then the queried data pairs $(x_i, y_i)_q$ will be the data pairs containing these invalid digital signatures. If the discrepancy-tracing procedure is being invoked because the tallier found overlap between L and RL, then the queried data pairs $(x_i, y_i)_q$ will be the data pairs affected by the overlap.

If all of the mix-net servers can generate satisfactory proofs of knowledge then the discrepancy arises, not with a mix-net server, M_j, but with the voter. Accordingly a different part of the discrepancy-tracing protocol (which presumes a cheating voter) is invoked, as will be discussed below with reference to Fig. 5.

If one of the mix-net servers cannot generate a satisfactory proof of knowledge, the discrepancy-tracing procedure of Fig. 4 continues, based on the presumption that the mix server which could not produce a satisfactory proof of knowledge is a cheating mix-server. This mix server is disqualified. The other mix servers in this mix-net, M, must now reveal their private keys, yielding SK_M. The c_i data recorded by the bulletin board server is now decrypted using SK_M and a new version of the list, L, is generated containing all of the decrypted data-pairs (x_i, y_i). This list, L, is sent to the tallier, TM.

In this case the tallier mix-net, TM, permutes the order of the entries (x_i, y_i) as well as decrypting the vote data. Moreover, in this case the servers, TM_j, of the tallier mix-net are prompted to generate respective proofs that they correctly mix and decrypt their inputs. This increases the duration of the vote counting phase, and increases costs. However, it is to be noted that the generation of these proofs is not required in the case of an election without irregularities. Once the vote data has been decrypted, it is counted and the tallier publishes the result of the election. This ends the counting phase.

Incidentally, if the randomizing module 40 served only to decrypt the signature-message pairs, and not to randomize their order, there would be a potential problem in the case where the servers of module 40 were obliged to reveal their keys (because of detection of an irregularity arising from operation of module 40). In such a case, when the keys were revealed there would be a direct correspondence between the first entry in the list, *L*, input to the module 40 and the first entry in the list of signature-message pairs output by the module 40. In view of the fact that the list input to the module 40 includes codes identifying the respective voters, this would prejudice the anonymity of the voting process.

On the other hand, if the discrepancy-tracing procedure of Fig. 5 has been invoked (in a case where it is presumed that the discrepancy arises from voter action, not action of servers in the randomizing mix-net), the normal operation of the tallier mix-net, TM, can be preserved, providing that the irregular vote data has been eliminated from the data to be processed.

More particularly, as indicated in Fig. 5, in the case of an irregularity attributable to a voter, the identity of the misbehaving voter can be revealed by implementing the back-tracing algorithm of the randomizing mix-net, M, using the queried data pair $(x_i, y_i)_q$. This will yield the identifier, Id_{ij} of the voter who sent the data c_{ij}, σ_{ij} to the bulletin board server, BB.

Once the misbehaving voter's identifier has been revealed, the signature-tracing mechanism of the fair blind signature scheme is applied so as to identify the data-pair (x_{ij}, y_{ij}) corresponding to Id_{ij}. This data pair (x_{ij}, y_{ij}) is added to the revocation list, **RL**, but removed from the list, **L**, of votes to be counted. The procedure can then return to Step 3 of Fig. 3.

It will be seen that, when there are no voting irregularities, the various mix servers do not need to generate proofs of the correctness of their operation. This leads to an extremely fast counting of the votes. Moreover, because misbehaving mix servers will always be detected in this system, it is unlikely that they will misbehave. Accordingly, the electronic voting scheme of the present invention is liable to yield the result of an election very rapidly.

Considering the security of the electronic voting scheme of the present invention, the following remarks can be made.

Provided that the digital signature scheme that is selected for use in the electronic voting scheme of the present invention is not capable of being broken, then the principles of eligibility and unreusability are respected in this scheme.

If at least one mix server is honest, and **n-t+1** of the trusted authorities are honest, then the anonymity of the voters is protected.

Advantageously, the preferred embodiments of the invention will be implemented using a digital signature scheme in which the signatures are one-more unforgeable as long as n-t+1 admin servers are honest. In such a case, a valid data pair (x_i, y_i) cannot be created. Thus the principle of accuracy is respected.

The talliers cannot decrypt the ballots during the progress of the counting phase because the tallier module is implemented as a mix-net. Therefore the principle of fairness is respected.

The voters do not need to take any special action to enable their votes to be opened, or to verify that their votes have been counted. Accordingly, the principle of "vote and go" is respected.

In the preferred embodiments of the invention, the lists $\mathbf{L}_{AS}$, $\mathbf{L}_{BB}$, **L** and **RL** are made public at the end of execution of the overall protocol. Moreover, every step of the counting stage (including the back-tracing procedures) can be published. This enables any interested party to check that the only ballots which have been discarded are those which truly were invalid, and to verify that the outcome of the election is consistent with the valid cast ballots. Thus, the principle of public verifiability is respected.

In the above-described process, it is preferred that the fair blind signature scheme should be a threshold fair blind signature scheme. Such schemes are well-known and so will not be described in detail here.

Although the present invention has been described in terms of a particular preferred embodiment thereof, the person skilled in the art will readily understand that various features of the preferred embodiment may be varied, adapted and/or replaced by others without departing from the present invention as defined in the accompanying claims.

For example, although the preferred embodiment has been described in terms of on-line voting, typically by users in their homes, it is to be understood that the physical location of the voters is unimportant – in some circumstances it is possible to envisage use of the present invention at a traditional polling station (which could, for example, be unstaffed).

Similarly, the present invention is not particularly limited with regard to the mechanism used for communicating the various signals between the participants in the system. Typically telecommunications networks and the internet will be used for communications between the users, the mix servers of the first mix net and the admin server. However, other networks can be used. In some circumstances it may be feasible for certain of the signals exchanged between the participants in the system to be recorded on a recording medium and physically transported between those participants.

It will be understood that the on-line voting techniques of the present invention can be applied in any kind of vote, whether it be an election, a referendum, an opinion poll, etc.